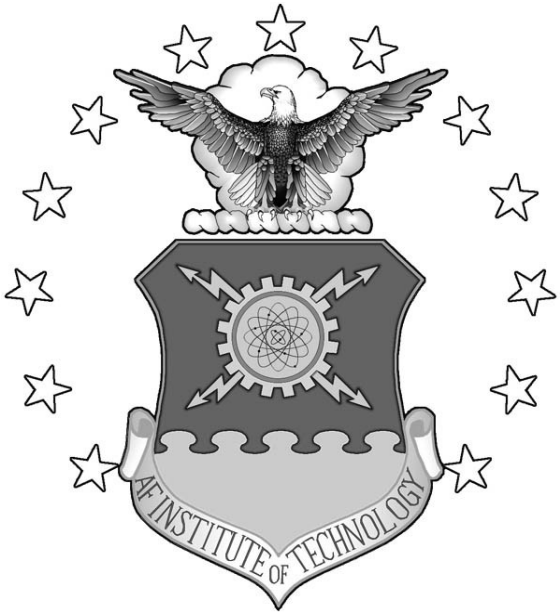


THE GREAT FIREWALL OF CHINA
A CRITICAL ANALYSIS

GRADUATE RESEARCH PAPER

Michael D. Whiting, Major, USAF

AFIT/ICW/ENG/08-12

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this graduate research project are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/ICW/ENG/08-12

THE GREAT FIREWALL OF CHINA
A CRITICAL ANALYSIS

GRADUATE RESEARCH PAPER

Presented to the Faculty

Department of Electrical & Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Cyber Warfare

Michael D. Whiting, BA, MBA

Major, USAF

June 2008

AFIT/ICW/ENG/08-12

THE GREAT FIREWALL OF CHINA
A CRITICAL ANALYSIS

Michael D. Whiting, BA, MBA

Major, USAF

Approved:

_____/signed/_____ _____

Robert F. Mills, PhD, USAF (Chairman) Date

_____/signed/_____ _____

Dennis D. Strouble, PhD, JD, USAF (Member) Date

AFIT/ICW/ENG/08-12

Abstract

Censorship has a great impact on society as we enter the cyber environment. The Chinese “Great Firewall”, as it is commonly called, brings great attention to China as they enter into the global economy. The Great Firewall is one approach China tries to censor their people. Many techniques are used to establish this cyber boundary such as: firewalls, real-name internet registration, filtering, political controls, police actions and governmental controls. These controls are being challenged by Chinese nationals through the mass public, technology, and software. There are many political, diplomatic, international, and non-governmental organizations who continue their efforts to minimize the affects of the Great Firewall. The United States finds itself in a unique situation trying to eliminate human rights violations while encouraging freedom. Some United States companies find themselves in a moral dilemma; accept the Chinese requirements to do business which may include supporting censorship and human rights violations or to eliminate doing business with the Chinese and missing out on a great financial opportunity.

To my devoted wife and two lovely girls for their support given throughout this year

Acknowledgements

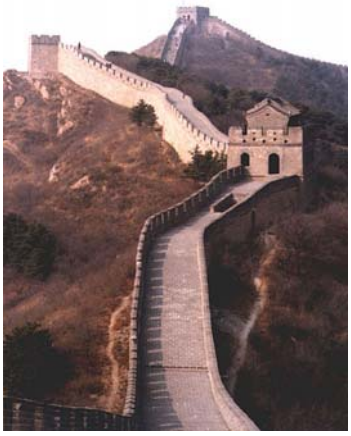
I would like to express my sincere appreciation to my classmates, family, mentors, and friends who gave me the opportunity to attend AFIT and make this an incredible year of learning. I want to give a special thanks to my advisor, Dr. Robert Mills, who has helped me throughout the year with advice, guidance and support, not only with the graduate research paper, but throughout the entire Cyber Warfare program. His efforts and passion for the future in cyber is infectious and I have learned a great deal from him. I'd like to thank Dr. Dennis Strouble for volunteering to advise on my research project. It has been a pleasure and you have shown me some great insight into the future of cyber law and the impacts it may have on the cyber issues, such as censorship. I would also like to thank Mr. Brendan Kelly from the Office of the Secretary of Defense, Policy, for his support and direction with this research project.

Michael D. Whiting

Table of Contents

AFIT/ICW/ENG/08-12

THE GREAT FIREWALL OF CHINA:
A CRITICAL ANALYSIS



(Source Unknown)

I. Introduction

Purpose

The Great Wall of China marked a period of time when the Chinese built a barrier against their enemies to defend their nation. A new barrier has been created, called the Great Firewall of China, which is a tool to censor all Internet activity coming into and out of China. A comparison will be drawn between the two to show reasons the Great Firewall may not be sustainable and how the Great Firewall of China may not be conducive to integration with free societies in a global economy. Many factors will be discussed related to censorship, human rights, democracy, and the global economy to make the case regarding the Great Firewall of China. This is important because China has had the largest economic growth than any other country in the past 25 years and their desire to be integrated with the global economy has brought great interest and tension to the global market.

This document will first outline the history of censorship in general terms and then discuss whether previous attempts were successful or not. Next, it will outline how China approaches censorship through the Great Firewall of China and their measures taken to ensure its success: politically, militarily, and financially. The third topic discussed will be the challenges that China faces through the authoritarian ideology in a global economy and whether it can be integrate successful with free societies. The next chapter will discuss the United States beliefs against censorship, the conflict with the current situation in China and what the U.S. should do regarding this situation that affects freedom, human rights, and the global economy.

The Great Wall of China

Several walls, collectively referred to as the Great Wall of China, were built since the fifth century BC. The most famous is the wall built between 220–200 BC by the first Emperor of China, Qin Shi Huang. Little of it remains, or it was much farther north than the current wall, which was built during the Ming Dynasty. The Great Wall at its peak was over 4,000 miles long and guarded by over 1 million men during the Ming dynasty.

The Great Wall of China was made of earth and stone and was built to protect China from northern invasions (Booth, 2008). The wall was constructed twenty five foot high, twenty foot wide and over 4,000 miles long when complete (Asimov, 1998). The wall was constructed sporadically, starting in 221 B.C. during the Chin Dynasty, and ending in the 1500's during the Ming Dynasty (Shea, 1998). Watch-towers were built every 200 yards and stood approximately 40 feet high (Booth, 2008). The top of the watch-towers were used for Chinese soldiers to spot any enemy movement, and the bottom of the tower was used to store food and military supplies (Valencia, 1998). The

Great Wall of China is the only man made object that can be seen from outer space with the naked eye (Booth, 2008).

Dynasty Political Decline

Centralization of government produced disastrous results. It brought the fear that now the emperor could do what ever he wanted. The major problem with an absolute emperor had been recognized long before the Ming dynasty: concentrating power in the hands of the emperor would spell disaster if the emperor were incompetent or disinterested in government. While incompetent emperors could come and go, the prime minister could guarantee a level of continuity and competence in the government. The Hong Wu emperor, wishing to concentrate absolute authority in his own hands, abolished the office of prime minister and so removed the only insurance against incompetent emperors (Hooker, 1996). The Ming dynasty was one series of unremarkable, mediocre emperors. This led to public scandals and dissention in the government between scholars and corrupt officials.

Ming Dynasty Rebellion

The political decline of the Ming dynasty began as early as the fifteenth century, but rebellions did not break out in the empire until the seventeenth century. Burdensome taxes were levied on the common people of China, largely to pay for extravagances at court and military expeditions against the Mongols and the increasingly aggressive Manchus. These taxes inspired rebellion, which led to a vicious circle of raising taxes to squash the rebellions through military force which required more taxes. The Manchus pressed their advantage (Hooker, 1996).

The Manchus

The greatest threat to the Ming, however, was the Manchus in the north. The Manchus were a stock of the Jurched tribe who lived in Manchuria. In the twelfth century, they founded a dynasty in Manchuria called the Chin ("Gold") dynasty; they were conquered a century later by the Mongols but became semi-independent during the Ming.

In the late 1630's, Abahai attacked North China; by this time, China was falling apart from rebellion. The major rebel leader was Li Tzu-ch'eng (1605-1645); he attacked Beijing in late April of 1644. Without much resistance, he entered the city on April 25 and the last Ming emperor, Ch'ung-chen, hung himself. The glorious Ming dynasty, so promising at its start, died on that afternoon. Thus began the last imperial dynasty in Chinese history: the Ch'ing or Manchu dynasty. This led to the end of the Ming and the Great Wall of China.

The Great Firewall of China

The Great Shield Project, also referred to as the Great Firewall of China, is a censorship and surveillance project operated by the Ministry of Public Security of the People's Republic of China. This project started in 1998 and began operations in November of 2003.

In 1998 the China Democracy Party was formed as one of the first true political opposition parties with global technical capabilities that could reach the masses via Internet, email and paging systems. The Communist Party feared the CDP would breed a powerful new network that would be difficult to control (Goldman, 2004). The CDP was

immediately banned followed by arrests and imprisonment (Goldsmith, 2006). That same year the Golden Shield project was started. The first part of the project lasted eight years, completing in 2006. The second part began in 2006 and should be completed by 2008. According to China Central Television, from 1998 to 2002, the project cost equivalent to $800 million dollars (Chinese Source, 2003).

II. Censorship

Censorship, defined by Encarta Encyclopedia, is the "supervision and control of the information and ideas that are circulated among the people within a society". In modern times, censorship refers to the examination of books, periodicals, plays, films, television and radio programs, news reports, and other communication media for the purpose of altering or suppressing parts thought to be objectionable or offensive. Examples of objectionable materials can include things to be considered immoral or obscene or material of any format that can seem to be injurious to society and/or national security. Rationale for censorship can often boil down to the social institutions of the family, church, and state.

In the past, censorship was established in various institutional forms up to the advanced democratic societies but by the mid-20th century, new social and societal attitudes weakened the strength of censorship in many democracies. In non-democratic societies censorship is a dominant and pervasive force, felt at all levels of artistic, intellectual, religious, political, public, and personal life. Hardly any act, expression, or relationship is exempt from official surveillance and accountability. (Konvitz, 2008)

The Universal Declaration of Human Rights, adopted the United Nations General Assembly in 1948, tries to set precedence to mitigate censorship in nondemocratic countries. The provisions of the declaration prohibit the interference with a person's home, family, privacy, or correspondence, and tries to provide the right to freedom of thought, religion, and expression without recourse. Thus, the worldwide struggle for human rights often involves problems of censorship as well as the fate of those dissidents who are its victims (Konvitz, 2008). This will be discussed in greater detail in later chapters.

Early History of Censorship

Censorship can be traced back to ancient times. It can be found in many societies because based on customs, culture and society, there are norms of behavior that are found to be accepted, enforced, or hidden from the society. The history of censorship will focus democratic states, religion, and government which will lead into the next chapter regarding China's beliefs on censorship and their impact on the global economy.

Greek and Roman Censorship

In Athens, a cradle of democracy, Socrates preferred to sacrifice his life rather than accept censorship of his teachings. Charged with the worship of strange gods and with the corruption of the youth he taught, Socrates defended free discussion as a supreme public service. He was thus the first person to formulate a philosophy of intellectual freedom. Ironically, his disciple Plato was the first philosopher to formulate a rationale for intellectual, religious, and artistic censorship.

Plato believed that art should be subservient to morality; art that could not be used to inculcate moral principles should be banned. In the idyllic state described in *The Republic,* censors would prohibit mothers and nurses from relating tales considered bad or evil; and in his *Laws* Plato proposed that wrong beliefs about God or the hereafter be treated as crimes and that formal machinery be set up to suppress heresy (Konvitz, 2008). This led to the philosopher Anaxagoras' punishment for impiety. Books were burned, and repression and persecution took over in Athens. This was a small phase where persecution took place; normally the Greek democracy was open to freedom of speech.

In Rome the general attitude was that only persons in authority, particularly members of the Senate, enjoyed the privilege of speaking freely. Public prosecution and punishment, supported by popular approval, occurred frequently (Konvitz, 2008). There was some religious tolerance toward other religions and cults during the Roman times. Religious freedom was accepted as long as the Roman Citizens worshipped the imperial person or image. Those who did not worship the imperial person were persecuted for their religious beliefs.

Censorship in the Modern World

The 18th century marks the beginning of the modern period, with its emphasis on toleration and liberty—a beginning that reflects the influence of the Age of Enlightenment and the American and French revolutions). This increase in tolerance first had an impact in religious beliefs but quickly led to political life. The Declaration of Independence (1776), the U.S. Constitution (1787) with its Bill of Rights (1789-91), and the French Declaration of the Rights of Man and of the Citizen (1789) became models for the modern world. In England Roman Catholics were freed in 1829; Jews achieved the same freedom in 1858 (Konvitz, 2008).

Modern democratic countries believe in the principles that religious beliefs, forms of worship are strictly for the individual and that government should not intrude on their religious freedom. Democracies believe that there should be a separation from government and religion. Communist countries such as the USSR, where religion was not at all, or only grudgingly, recognized, and atheism was the established ideology (Konvitz, 2008). The Communist countries did not allow for freedom of religion and often persecuted those of different beliefs.

Government Censorship

State censorship remained severe in the Soviet Union and other countries where political opposition was suppressed by permitting the existence of only one party. In these situations violations that breached the political or moral boundaries, could result in punishment by fines, imprisonment, restriction on publication, or closing the medium of communication. Examples of this are present in the current Chinese Great Shield program.

Rating countries on a scale ranging from 1 (most free) to 15 (least free), a survey published by Freedom House in the late 1980s disclosed that 60 countries comprising about 2 billion people enjoyed the highest degrees of freedom (1-5). In these countries—which were concentrated in North America, Western Europe, Japan, Australia, and New Zealand—individuals generally had the right to bring about peaceful changes in government, enjoyed freedom of speech and press, and had free access to other mass communications. Another 39 countries with about 1 billion people received rankings of between 6 and 10. Finally 68 countries with roughly 2.1 billion people had forms of government that denied citizens most political and civil rights. (Konvitz, 2008)

Authoritarian Regimes Censorship

Authoritarian regimes are finding ways to control and counter the political impact of Internet use. In Singapore, a long-standing semi-authoritarian regime is implementing an ambitious yet carefully planned strategy, using a combination of legal, technical, and social measure to shape the development of Internet use (Rodan, 1998). In military-run regimes such as Myammar, Burma, governments can curtail dissident communication by

preventing popular access to the Internet and forbidding use of other mediums such as fax machines and satellite dishes (Kalathil, 2001). And while much attention has focuses on the role of Internet-coordinated student protest in the downfall of Suharto in Indonesia, analysts have found it hard to draw a causal link between protestors' use of technology and regime change (Kalathil, Boas, 2001).

Current Problems and Trends

As can be seen throughout history, restrictions have been placed on individuals and societies to restrict the flow of information, freedom of belief, and freedom of religion. These restrictions have been successful for short periods of time. Censorship has many social impacts on society's religious, political, and economic freedoms and is increasingly difficult to control in today's new information age.

In the 20th century freedom from censorship has been the exception in the world. The rule has been, and continues to be, repression, suppression, and oppression (Konvitz, 2008). It may be a sign of progress that many countries say they are committed to liberty and that they oppose a policy of religious, intellectual, or political censorship.

Throughout time there are many examples where people either 1) know that censorship is taking place and don't care, 2) know that censorship is taking place and care about it, 3) don't know censorship is taking place and would care if they knew it was taking place, 4) don't know censorship is taking place and wouldn't care if they knew about it. Any of these situations impact how aggressive a society will fight to overcome the censorship against its society.

The trend is that over time censorship will be overcome by the will of the people as the society develops into a diplomatic state with the focus on freedom. This is no easy

process. In history it can take decades or centuries to change the political beliefs of a society but in today's world with the vast availability of information and technological advances it is difficult to enforce censorship. Diplomatic states are very involved to ensure that human rights issues are not overlooked and that freedom is promoted world-wide.

Finally, the Internet has the potential to challenge the stability of authoritarian regimes. In cases where Internet use appears threatening, states will respond and even try to preempt these challenges, seeking to maintain control over the Internet as they have with other media in the past. These responses are likely to involve a combination of two types of strategies: reactive and proactive. Reactive strategies are the most visible, involving direct efforts to counter or circumvent the potential challenges outlined above by clamping down on Internet use. Included in this category are strategies such as limiting access to networked computers; filtering content or blocking Web sites with software tools; monitoring users' online behavior; or, even prohibiting Internet usage entirely (Kalathil, Boas, 2001). Now we will talk specifically about China's approach to censorship.

III. China's Approach to Censorship

The Chinese government actually controls the Internet within their country, and other forms of media productions such as television and radio. The People's Republic of China government has recently intensified censorship measures. The Great Firewall of China has been established and has been quite successful but can it be sustained over time?

Internet usage has grown rapidly in China. According to the latest survey from the official China Internet Network Information Center, there were about 168 million internet users in China by the end of June 2007, and an estimated 122 million Chinese have broadband access to the Internet. Compared with the estimated current Internet population in the United States, which ranges from 165 million to 210 million users (Xiao, 2007). Also, a related and even more phenomenal growth in the mobile phone market in China has taken place. Currently there are more than 440 million mobile phone users in China, many of whom carry phones with wireless and text messaging (Xiao, 2007). Recent indications state that China has overtaken the United States in total number of Internet users.

Political Controls

Since the introduction of the Internet in China, the government has been very ambivalent towards this new force in Chinese society: on the one hand, it considers both the Internet and Information and Communication Technologies (ICT) generally as essential parts of the country's economic development, and has actively (and successfully) supported online businesses and e-government projects. On the other hand, it has consistently and tirelessly worked to improve and expand its ability to control

online speech and to silence voices that are considered too provocative or challenging to the status quo (Xiao, 2007).

In early 2007, in a talk to the Political Bureau of the Central Committee of Communist Party of China, President Hu called on government authorities to strengthen Internet controls stating, “Whether we can cope with the Internet is a matter that affects the development of socialist culture, the security of information, and the stability of the state.” Hu called on officials to improve the technologies, content controls and network security that are used to monitor the Internet (Xiao, 2007).

The government of China uses many different techniques to control online content. The use a combination of people process and technology: technical filters, regulations and administrative rules, Internet police forces, and, above all, self-censorship from both website administrators and users. These techniques will be discussed briefly.

Several political bodies are in charge of developing and monitoring the Internet content within China. The most important are the Central Propaganda Department, which ensures that media and cultural content follows the official standards as mandated by the Communist Party and the State Council Information Office (SCIO). The Central Propaganda Department is very secretive about their operations and does not have a website or share public information about their office. The SCIO is an official office of the State Council. It oversees all websites that publish news, including the official sites of news organizations as well as independent sites that post news content. Counterpart offices at the provincial and city levels have also been established. Every provincial and city government has “information and publicity” offices, as lower level counterparts to SCIO’s national-level Bureau. All of these offices together comprise a vast and rather effective network that monitors online information and controls online content. The SCIO

is also responsible for China's "perception management" to the international community (Xiao, 2007).

The Ministry of Information Industry (MII) oversees regulation of the telecommunications and software industries. MII is primarily responsible for the construction and management of China's Internet infrastructure. The government website defines the MII as "a regulatory body in charge of the manufacture of electronic and information products, the communications and software industry, as well as the promotion of informatization of the national economy and social services in the country" (Xiang, 2007). The MII is also responsible for licensing and registering all websites in the country. This office also has the responsibility of building the surveillance and filtering technologies is collectively known as The Great Firewall.

The Ministry of Public Security, the national law enforcement agency under the State Council, is responsible for monitoring online content and using law enforcement powers to arrest those who violate the regulations. The Ministry of Public Security established the "Public Information Internet Monitoring Bureau" in 2000, with sub-divisions at every provincial and municipal level. Internet police forces monitor websites for "illegal" content, and can order hosting service companies to warn or shut down an offending site. Internet police are responsible for the following tasks: implementing Internet control policies; together with the MII, developing surveillance and encryption technologies; monitoring online content; forbidding non-media websites from using reporters and publishing independent news content; preventing foreign capital from controlling mainland media; strictly reviewing the licensing process for Internet companies and websites, particularly focusing on information which potentially "threatens national security"; preventing people from using the Internet to organize and

mobilize collective actions; and finally, blocking certain overseas online content (Xiao, 2007).

Internet Censorship Techniques

Government

As discussed in previous section, many state agencies control the Internet in China. They censor content transmitted through Web pages, blogs, forums, bulletin boards and e-mail. Media regulation and state secrets laws, cybercafé regulations, and controls over service and content providers are designed to support filtering. The Central Propaganda Department and the SCIO make sure content providers adhere to material that is consistent with Communist Party ideology.

Businesses

Western corporations provide much of the equipment and services for China's Internet system. Major players include Cisco Systems, Nortel Networks, Sun Microsystems, 3COM, Google, Yahoo!, Microsoft, IBM and others. Yahoo! and Google agreed to rework their search engines to comply with China's filtering practices. Cisco Systems has been integral to China's Internet development. Its router equipment, which reportedly provides no anonymity or encryption and was specifically designed for China, is in the core of the nation's surveillance of the Internet.

Providers

Internet Service Providers (ISPs) must track who is online and what web sites are visited. Customers' account numbers, phone numbers and IP addresses must be kept on file. ISPs can be held legally responsible if customers use their systems to violate laws.

Internet Content Providers (ICPs) that publish content and operate bulletin boards are legally responsible for content appearing on their sites. ICPs must also set up systems of secure registration and login to be able to verify users' identities and track their online activity. If they fail to do so, their business licenses will be revoked and the company's staff could be prosecuted.

Cybercafes

Called wangba, or Net bars, cybercafés are required to keep detailed logs of customers' online activity on file for 60 days. If a user tries to access forbidden Web sites, a café must disconnect the user and file a report with state agencies. Penalties for violations include fines and even imprisonment. People cannot use cyber services without an identification card, which is kept on record for at least 60 days. Children under 16 are not allowed in cybercafés, where people often play violent video games.

People

Every Chinese person, who signs up for Internet service, must register their Internet information with his or her local police department within 30 days. Volunteers, guided by ISP employees, monitor Web sites, chat rooms and bulletin boards to prevent prohibited language from being published. Civilians may report violations to the authorities. Volunteers also clean up postings by deleting any that manage to evade automatic filters.

E-mail

The Chinese keep a close eye on communication tools such as e-mail. E-mail is filtered by service providers. The method is based on the same technology that blocks

spam. Body text and subject lines are scanned and blocked if anything objectionable is found.

Keyword

Chinese search engines monitor content by keyword and remove offending Web sites. When people request banned content through Chinese search engines like Baidu and Yisou, the filtering system disconnects them.

Blogs, discussion forums, and bulletin boards are very popular in China. They're heavily filtered by keyword blocks. Blogs' service providers do not let posts with certain words be published, and blogs are also censored manually.

Here's a short list of keywords that will trigger the filtering system and block access to content: Revolution, Equality, Freedom, Justice, Taiwan, Tibet, Falun Gong, Dissident, Democracy, STD, and Human rights.

URL/Domain name

Internet content is also filtered by domain names and URLs, or Internet addresses, which are blocked if they contain words or combinations of letters similar to those on the list of blocked topics.

IP Addresses

Blocking by Internet Protocol (IP) address creates even stronger barriers to information. Because a Web site can be reached by a URL or an IP address, China blocks both with technology and tricks such as TCP connection termination and "ZeroWindow" condition.

Web sites

The Chinese government blocks Web sites of some Western media outlets and human rights organizations -- and any it deems politically or socially harmful. Chinese

people trying to access information related to Taiwanese and Tibetan independence, the Dalai Lama, Tiananmen Square, SARS, opposition political parties, and anti-Communist movements will find themselves out of luck. Information about any group that can organize large numbers of people is considered threatening.

IV. China's Big Challenges

Potential Challenges

Despite disagreements within the government as to strategy, the top leadership continues to see the development and promotion of the Internet in China as a tool for economic development, with the understanding that at some level this modernization will help consolidate popular support for the current regime (Kalathil, 2001). Yet as the Internet develops in China, its interactive nature implies even greater challenges in balancing economic potential and political control. China's big challenge is maintaining control over the Internet's political impact through reactive and proactive strategies.

States proactively guide Internet development and usage to promote their interests and priorities. While reactive strategies respond to existing or potential challenges of Internet use, proactive strategies attempt to develop an Internet that is free from such challenges while also extending state authority. These strategies may involve efforts to distribute propaganda on the Internet, both domestically and internationally; build state-controlled national Intranets that serve as a substitute for the global Internet; implement e-government services that increase citizen satisfaction with the government; and even strengthen state power on an international scale by engaging in information warfare, such as hacking into Web sites and spreading viruses. In addition, governments may harness the Internet to serve economic development goals, with an understanding that economic growth and a general increase in the standard of living may also help shore up public support for the current regime.

Reactive State Responses

Most of the speculation about the Internet's political effects in China concerns its impact on the mass public. Because it allows access to multiple sources of images, news, and ideas some believe the Internet can challenge state hegemony over the distribution of information and ideologies. (Taubman, 1998) China's people are becoming extremely educated and are becoming increasingly aware of foreign products, culture, and political norms. Through this increased awareness, often through Internet chat-rooms, there are lively discussions regarding situations like the downed U.S. surveillance plane that went down on Hainan Island or the schoolhouse explosion in Jiangxi province that are both positive and negative regarding the government. Some believe that direct involvement in such forums will lead to the political liberalization of the state. Chat room administrators hire censors to screen and quickly remove offensive material from bulletin boards. Indeed, during the schoolhouse blast incident in March 2001, these censors immediately deleted all chat-room comments thought too politically sensitive or critical of the government (Lee-Young, 2001). These type actions continue today.

In response to international uses of the Internet for political advocacy, China has engaged in its own propaganda campaigns, posting counter-information on government and government-sponsored Web sites to influence both domestic and international opinion. Overseas practitioners of Falun Gong also contend that the Chinese government uses information warfare techniques - such as hacking into Web sites and spreading viruses - to disable and discredit their organizations (Kalathil, 2001).

Finally, the Chinese state faces a number of internal challenges to Internet governance. At present, over twenty party and government organizations consider the Internet part of their bureaucratic domain, and both local and national arms of state

bureaucracy have commercial interests in promoting the new technology (Goodman & Foster, 1999). Power struggles and turf-grabbing by various ministries have at times curtailed the state's ability to effectively govern the Internet. In addition to these conflicting interests, inefficiencies and lack of communication among bureaus can also hamper effective state control of the medium (Mazurkewich, 2000). In part, the state's response to its own internal divisions has been a reactive one, as the top leadership seeks to consolidate ministries and curtail local decision making. But the state is also responding to these internal challenges by implementing a number of proactive e-government strategies, as detailed below.

Proactive State Responses

China's reactive methods of controlling the Internet have received the most international attention, but the leadership has also developed a number of equally significant proactive strategies designed to leverage the Internet to strengthen the Chinese state. Through both overt measures (such as e-government procedures and the design of a nationwide Intranet) and more subtle means (such as channeling online discourse in ways that support the regime), the Chinese state has shown that it can use the Internet to enhance the implementation of its own agenda.

In addition to distributing propaganda on the global Internet, China is reviving the idea of a national Intranet, which will be designed to substitute for the global Internet by providing online services paired with acceptable content (whose exact nature has yet to be detailed) for Chinese citizens (Kalathil, Boas, 2001). Even though this plan has been discussed for years, the emphasis that has been put on the Great Firewall shows the state’s worry and continued efforts to stop the infiltration of foreign ideas.

Another proactive strategy is the promotion of Internet development in the hopes that economic modernization will increase the regime's popularity and political legitimacy. As Yi Feng has argued, the likelihood of short-term political upheaval is lower in authoritarian regimes that are perceived to have increased living standards and promoted economic growth (Yi, 1997).

Finally, the Chinese government is developing a strategy for information warfare that will allow it to more effectively project its power on an international scale. Recent writings Chinese military specialists show that China is increasingly focusing on “asymmetric warfare” options, including guerrilla war and cyber attacks against data networks (MacDonald, 2004). In recent years, U.S. experts believe that China is willing to reduce its standing army while increasing its reliance on a "multitude on information engineers and citizens with laptops instead of just soldiers" (Thomas, 2004). Although Chinese hacker attacks on U.S. Web sites in May 2001 did not demonstrate the offensive capacity Chinese military analysts have envisioned, the continued study and development of information warfare can be seen as a top-priority proactive measure in line with the country's goal of modernizing and transforming its military strategy. We have learned since then that the Chinese military continues to train and develop their strategy to focus on asymmetric warfare.

Mass Public

The common people of China can impact the governmental controls of the Internet and the effects of Censorship. Exposure to outside ideas and images from

diplomatic societies can lead to rebellious attitudes to seek ways to get around the Internet censorship and eventually lead to political changes, if not an outright regime change. This would not be an easy process and will take a sustained, long-term effort.

Civil Society Organizations

Many social organizations put great pressure to change the rules that an authoritarian state puts on there people, especially when it involves human rights issues. Organizations such as Human Rights Watch Organization continue to fight for the rights of the people of China.

Global Economy

With the great efforts China is making to engage in the global economy, they are pursuing ways to effectively utilize the internet to their economic advantage. Here may be the biggest problem that China will face trying to keep their Great Firewall functional. The pursuit of the global economy and the potential for economic growth can place forces on the society to challenge the governmental controls (Lehrer, 06).

International Community

The international community can put political and economic pressures on China to loosen up their governmental controls to encourage fair trade and to eliminate perceived human rights violations. This can be done through many different measures such as imposing sanctions and trade embargos.

Technology

As reported from Online Newshour: China Internet Censorship transcript, a Chinese-born computer scientist, who doesn't want his identity revealed, is waging a technological war on the Chinese government. He is working to improve a software program he designed that people in China can use to get around their government's Internet censorship. A group of his friends has invented a technology that can breakthrough China's great firewall so that it enables Internet users in China, can visit any Web sites from the United States or from other free world.

The technology, which masks the Web sites visited, is called Ultrareach. It uses both encryption and a constantly changing computer identification that allows access to banned Web sites. He stated, “I don't think China government likes it. You know, they see the Internet as a threat in the freedom of the information expression. One of his partners on the software has allegedly been beaten up for his involvement with the project.”

One hundred and fifteen million Chinese go online only to find that the government uses filters to block sites that provide information about democracy or the uprising in Tiananmen Square or dissident groups. In order to get around those restrictions, more than 100,000 Chinese uses Ultrareach and other technologies every day, which in turn has led authorities to fight back, inventing new technologies and buying foreign programs to foil the anti-censorship software.

Proxy relays

People use proxy relays to get around Internet filtering and monitoring. A proxy server acts as a buffer between a Web browser and a Web server. Proxy manipulation allows users to connect to the Internet through servers based abroad.

Software

Many different kinds of software allow users to surf the Internet anonymously and protect their privacy. The so-called anonymous communications systems hide a user's identity from the content provider.

Circumventors

Web-based circumventors are special Web pages in which a user can enter a blocked URL in a special form and press the "submit" button. The circumventor pulls the content and displays it. With a Web-based circumventor, no software has to be installed and no browser setting must be changed.

Tunneling

Tunneling allows a user in a censored location to access information through a tunnel to a computer in an unfiltered location. All requests run through an encrypted tunnel to a non-filtered computer, which forwards requests and responses transparently. Both private and commercial tunneling services are available.

Other techniques

Many other creative techniques bypass censorship. Another well-known method of ad-hoc circumvention is accessing Google's cache. Google's cache function sends search requests to its regular servers and not to the blocked source's servers.

Mass Public

On the Berkeley campus of the University of California, Xiao Qiang directs the China Internet Project and advocates for a freer Internet policy. Qiang says the Chinese government encourages the use of the Internet for its economic benefits in a global

economy. On the one hand, we see this very rapid development of the Internet infrastructure, the practices. And on the other hand, we also see these unprecedented, enormous resources being put into the control, the filtering, the monitoring, the censorship, and surveillance, what we call altogether China's great firewall.

> "The Chinese have a millennial tradition of censorship and of literary inquisitions. Frederick Wakeman, professor of history and Asian studies at Berkeley, says the Chinese have long tried to limit information, and rebels have always tried to circumvent censorship. He thought the Internet might change things. I think, when it first appeared, we thought, well, this is going to open up channels of communication that the Chinese themselves cannot control. I can remember, back in the days when the fax machine was first introduced, and I would send a fax from Peking, and there would be a Chinese security officer at my elbow to make sure the fax was secure. They had enough manpower to do that. Now, they obviously are trying to extend that into the area of the Internet, which is much more difficult. The Chinese will find ways to get around it. There are also people that use circumventers to get around the Great Firewall."

V. What should the U.S. do?

National Security Strategy

The National Security Strategy of 2006 goal is to seek and support democratic movements and the institutions in every nation and culture, with the ultimate goal of ending tyranny in our world.

First pillar is "promoting freedom, justice, and human dignity – working to end tyranny, to promote effective democracies, and to extend prosperity through free and fair trade and wise development policies". A key component of this is to "Champion aspirations for Human Dignity". The United States Government will work to advance human dignity in word and deed, speaking out for freedom and against violations of human rights and allocating appropriate resources to advance these ideals.

Another pillar of the National Security Strategy is to "Ignite a new era of global economic growth through free markets and free trade". The final pillar of the National Security Strategy that will be discussed is the need to "Engage the opportunities and confront the challenges of globalization".

In authoritarian regimes the state has played a strong role in the development and control of the mass media which carries right into the internet development of the Chinese people. In contrast, democratic governments find themselves struggling to impose effective regulation and over sight over the same medium.

The Internet poses unique challenges for those who would try to hamper free expression as well as for those who campaign to defend it. Because the technology for disseminating information has evolved so quickly (now including increasingly sophisticated peer-to-peer networks for sharing data), legislation finds it hard to keep up with the possibilities for expression made possible by this medium. However, security

devices, sometimes implemented in conjunction with government efforts to suppress free speech, as in the case of China's "Golden Shield", can limit user' access to certain kinds of content and make startling infringements on their privacy (NCAC.ORG, 2008). So what, if anything, should the United States do in regards to China's Great Firewall and censorship issues?

Censorship in the United States

When the American colonists drafted laws before 1776, they borrowed from English precedents regarding personal rights and liberties but went far beyond Great Britain in the fields of freedom of religion, speech, press, and assembly. After the American Revolution and the adoption of the U.S. Constitution, these freedoms were guaranteed in the Bill of Rights, the first ten amendments to the Constitution (Konvitz, 2008). Although it is not explicitly stated our personal rights and freedoms extend to protection from censorship. The First Amendment, in broad terms, forbids Congress from enacting laws that would regulate speech or press before publication or punish after publication.

There is a growing consensus among politicians and pundits in the United States that the Internet poses an insurmountable threat to authoritarian regimes. President Bush has asserted that the Internet will bring freedom to China, while Secretary of State Colin Powell recently stated that "the rise of democracy and the power of the information revolution combine to leverage each other." Members of the Clinton administration were also prolific proponents of the idea that the Internet is inevitably a force for democracy. Business leaders and media commentators usually concur, and voices to the contrary have been few and far between (NCAC.ORG, 2008).

A flourishing “marketplace of ideas” is one of the great goals of the First Amendment. It is jeopardized today by an environment of government secrecy that denies the public and even lawmakers access to information necessary to make sound decisions. Without question, some information must be safeguarded in the interest of national security. Nevertheless, review by courts or legislators are essential to ensure that national security is not invoked unnecessarily, or merely to keep potentially incriminating or embarrassing conduct under wraps. Some recent revelations justify public skepticism (NCAC.ORG, 2008).

US Companies/Issues

In the last two decades, the Internet has grown at an incredible rate and has rapidly become more accessible to people of all walks of life, throughout the world. Google now claims to index over 3 billion Web sites. It is no surprise, then, that the “information superhighway” has become an especially heated battleground for free speech (NCAC.ORG, 2008). Google and Yahoo! have both made configuration changes to comply with China’s filtering practices and to comply with the local laws.

Yahoo!

The revelation comes a day after one of the major internet players, Yahoo!, asked a US court to dismiss a lawsuit accusing it of complicity in human rights abuses in China. The World Organization for Human Rights is suing Yahoo! for sharing information about its users with Chinese state officials. Information gathered from Yahoo’s Chinese subsidiary has led to the arrests of writers and dissidents, including journalist Shi Tao who was tracked down and jailed for 10 years for subversion after his e-mail and IP

address were passed to the Government. Yahoo! maintains it has no case to answer as it must comply with local laws. Many websites are eliminated from Yahoo! and Google in China, but both argue it is better to offer Chinese users some information than none at all (Groves, 07).

Yahoo! executives respond consistently that search engine filtering is done in compliance with Chinese law, and that there is no alternative other than not doing business in China at all. In May 2006 Yahoo! CEO Terry Semel responded that providing the censored and politically compromised services still benefits the Chinese people more than if Yahoo! were absent from China altogether.

Yahoo! continues to defend itself against charges that its Chinese operations have been responsible for the jailing of multiple dissidents. Multiple reports have surfaced which tie Yahoo! Mail to various Chinese court cases that have ended in imprisonment for writers with politically unpopular opinions.

It's not just Yahoo! that has come under scrutiny for its Chinese operations, though. Both Microsoft and Google have also endured their share of criticism for decisions each has made to give in to government-ordered censorship. These companies are trying to walk a fine line between offending the Chinese government, on the one hand, and offending the American government on the other. The US Congress has gone so far as to hold hearings on the issue, though so far has done little to hinder US businesses in China. Because Yahoo's actions have led to jail time and not simply censorship, the company has received the most criticism and is regularly asked about its practices in China. The general response from Yahoo! is that it has to comply with local laws, just as it does in the US, and that even a censored Internet is better than no Internet at all. Yahoo! CEO Terry Semel reiterated that stance in a recent New York talk. "You

have to get whatever news you possibly can into China as opposed to pulling back," he said. "Will they be edited? Yes. Should you go home? No." He went on to say that Yahoo! cannot change Chinese policy and that it needs help from the US government to do so. Unfortunately, much of the news available inside China is heavily censored by the countries so-called Great Firewall, and Xinhua, the country's offical "news" organization; generally does little more than rehash wire reports and Communist Party press releases from a pro-government perspective (Anderson, 06).

Google

While Google has had a Chinese language search engine since September 2000, the company did not set up a physical presence inside the People's Republic of China until the launch of its Beijing research and development center in July 2005 (Associated Press, 2006).

In December 2005 Google received its license as a Chinese Internet service and Google is engaged with active censorship in China. Then on January 26, 2006, Google launched a censored version of its search engine for the Chinese market in which Google became the censor, not merely the victim of state and ISP censorship. Tests of the site showed that Google.cn censors thousands of keywords and web addresses. The "block list" was not given to Google by the Chinese government, but rather—as with the other search engines operating in China—was created internally by Google staff based on their own testing of what terms and web addresses were being blocked by Chinese Internet service providers (Thompson, 06).

Google's CEO Eric Schmidt explained that Google's decision to launch a censored service was the result of a great deal of internal wrangling within the company,

but that ultimately Google executives concluded that censorship was necessary for Google to provide more and better service to Chinese Internet users. “We concluded that although we weren’t wild about the restrictions, it was even worse to not try to serve those users at all,” he said. “We actually did an evil scale and decided not to serve at all was worse evil.” (Sullivan, 06).

Cisco

Cisco Systems has been integral to China's Internet development. Its router equipment, which reportedly provides no anonymity or encryption and was specifically designed for China, is in the core of the nation's surveillance of the Internet. (Sources, 2007)

An internal Cisco document leaked to reporters on the eve of a Senate human rights hearing reveals that Cisco engineers regarded the Chinese government's rigid internet censorship program as an opportunity to do more business with the repressive regime. The 90-page document is an internal presentation that Cisco engineers and staffers in China mulled over in 2002 as the central government was upgrading its local, state and provincial public safety and security network infrastructure. Under the category "Cisco Opportunities," the document provides bullet point suggestions for how it might service China's censorship system called the "Golden Shield” and better known in the West as the Great Firewall of China. China’s Golden Shield project was one of several government-run commercial opportunities for Cisco in 2002. (Stirland, 2008)

The document is the first evidence that the networking giant has marketed its routers to China specifically as a tool of repression. It reinforces the double-edged role that Americans' technological ingenuity plays in the rest of the world. (Stirland, 2008)

Global Economy

An open-market system certainly doesn't mitigate against a more open society and open political environment, but one would be somewhat naive to assume that, ipso facto, it leads to it. News reports say the Chinese employ at least 30,000 Internet police. And according to human rights groups, between 42 and 87 people have been jailed for Internet crimes. In the past twenty years of economic reform, it has not led to certain kinds of critical political openness. So, there are other elements that need to be brought online, and that's the willingness of leaders to be able to have countenance for political reform and they're very wary of it because they are trying to maintain social stability in China. They see an open media, a greater quotient of rights, as being a real threat to their ability to keep economic progress going and to keeping the society as a whole on a relatively even keel (Sources, 2006).

Chinese Military

The Chinese military doctrine critically centers on the traditional superiority of a people's war. As China once again strengthens its people's war, this time it is not drawing in the enemy to the mainland, but without contact, intangibly fighting, with offensive character in the information space (Ryou, 08).

China's goals are more subtle but no less dangerous. Although the Chinese government has denied involvement in this latest round of attacks, government officials last year published a report entitled "China's National Defense in 2006" that states China is pursuing a three-step development strategy to modernize its national defense and

armed forces that includes building “informationized armed forces” capable of winning “informationized wars” by 2050.

The potential for information warfare was a key component of the U.S. Department of Defense's report to Congress earlier this year analyzing China's military capabilities. China views the acquisition and effective distribution of data as crucial to its ability to optimize “materials, energy and information to form a combined fighting force” and to apply “effective means to weaken the enemy side's information superiority and lower the operational efficiency of enemy information equipment,” the report says (Greenmier, 07).

VI. Conclusion

It is widely believed that the Internet poses an insurmountable threat to authoritarian rule. Although some political science scholars believe that authoritarian regimes are finding ways to control and counter the use of the Internet, the pressures and influence of the international community, political pressures, expansion of the global economy, and maybe most importantly, the people of China will greatly influence the control of the Great Firewall of China.

Until now, the Chinese government has been quite effective in controlling the political impact of the Internet by developing a multi-layered strategy to control Internet content and monitor online activities at every level of Internet service and content networks. The government still possesses enormous resources for social control in preventing online public opinion leading to collective action in real space.

However, beneath the surface of these constantly increasing and intensified control measures, there is a rising level of public information and awareness in Chinese society, facilitated by information and communication technologies, particularly cell phones and the Internet. The erosion of the Party's old ideological and social control is underway, as recent news events, from environment protests in Xiamen to Shanxi brick kilns vividly demonstrated. The long-term implications of this process can have profound and far-reaching consequences, for Chinese society as well as for China's relations with the U.S. and other countries.

The U.S. has many factors to consider in how it handles relations with the Chinese government. First, the U.S. must decide if the Great Firewall possesses a threat to our national interests. Then the U.S. must decide how to deal with China's censorship

and human rights violations while China engages the Global Economy. Finally, The U.S. needs to enforce laws on U.S. companies that choose to do business with China and directly assist and enable the censorship and human rights violations of the Chinese people by doing business with the Chinese government without concern of legal prosecution.

The Great Firewall of China is currently rather effective but through technological advances and the will of the people, the Chinese and the international community will find ways to overcome the effectiveness of the Great Firewall.

Bibliography

Anderson, N (2006, May). Yahoo on China: We're doing some good. *ars technica*, Retrieved 5.23.08, from http://arstechnica.com/news.ars/post/20060512-6823.html

Asimov, I (1998). Construction of the great wall. Retrieved May 20, 2008, from Great Wall Web site: http://www.ccds.charlotte.nc.us/History/China/save/barrett/barrett.html

Associated Press, (2006, April 12). Retrieved May 23, 2008, from Google defends cooperation with China Web site: http://www.msnbc.msn.com/id/12283735/

Booth, H. (2008). Defense from attack: The great wall of China. Retrieved May 20, 2008, from Web site: http://hermes.bryant.edu/Humanities/HUM101/Text/greatwall.html

Chinese Source (2003). Retrieved on May 20, 2008, from Internet: http://en.wikipedia.org/wiki/Golden_Shield_Project

Goldman, M (2004). *Chinese Intellectuals between State and Market*. Routledge publishing.

Goldsmith, J (2006). *Who controls the internet?: Illusions of borderless world*. Oxford university press.

Goodman, S. & Foster, W. (1999). The internet in China and India. *Internet Society, 1999*, Retrieved Mar 17, 08, from http://www.isoc.org/inet99/3a/3a_3.htm

Greenemeier , Larry (2007, September 18). China's Cyber Attacks Signal New Battlefield Is Online. Retrieved May 12, 2008, from www.sciam.com Web site: http://www.sciam.com/article.cfm?id=chinas-cyber-attacks-sign&ref=rss

Groves, Paul (2007, Aug 29). Retrieved May 12, 2008, from Yahoo, internet censorship, chinese cyber police and the olympics Web site: http://grovesmedia.wordpress.com/2007/08/29/yahoo-internet-censorship-chinese-cyber-police-and-the-olympics/

Hooker, Richard (1996). Ming China; The decline of the Ming. Retrieved May 12, 2008, from http://www.wsu.edu/~dee/MING/DECLINE.HTM Web site: http://www.wsu.edu/~dee/MING/DECLINE.HTM

Kalathil, S (2001). The internet and asia: Broadband or Broad Bans?. *Carnegie Endowment for international peace, 78*, Retrieved May 20,2008, from http://www.carnegieendowment.org/publications/index.cfm?fa=view&id=621

Kalathil, S, & Boas, T (2001). The Internet and State Control in Authoritarian Regimes: China, Cuba, And the Counterrevolution. *First Monday, 6*, Retrieved May 19, 2008, from http://www.firstmonday.org/issues/issue6_8/kalathil/.

Konvitz, Milton Censorship. (2008). Censorship. In *MSN Encarta* [Web]. Retrieved 5/12/08, from http://encarta.msn.com/encyclopedia_761559522/Censorship.html

Lee-Young, J (2001). Beijing cracks down on firecracker scandal. *Internet News for Internet Business*, Retrieved Jun 20, 2001, from http://ww6.infoworld.com/article/0,1902,22879,00.html

Lehrer, J. Transcript (2006). Chinese Internet Censorship. *Online NewsHour, April 2006*. Retrieve 5/23/08, from http://www.pbs.org/newshour/bb/asia/jan-june06/china_4-18.html

MacDonald, E. (2004, Sep) "The Same, Only Different: Just War Theory, International Law, and Traditional Chinese Thought" *Paper presented at the annual meeting of the American Political Science Association, Hilton Chicago and the Palmer House Hilton, Chicago, IL* Online <.PDF> Retrieved 2008-04-21 from http://www.allacademic.com/meta/p61063_index.html

Mazurkewich, K (2000). "Making a play: Global portals prepare to move into China as Beijing Appears to relax its internet rules. *Far Eastern Economic Review, August, 2000.*

NCAC.ORG, *A presumption in favor of secrecy, #106*, Retrieved 5/12/08, from http://ncac.org/censorship_news/20080205~cn106~A_Presumption_in_Favor_of_Secrecy.cfm

Ryou, Hayoun (2008, Jan 22). Chinese cyber war. *IDSA institute for defence studies & analysis*, Retrieved 5-12-08, from http://www.idsa.in/publications/stratcomments/HayounRyou220108.htm

Shea, M. (1998). The Great Wall of China. 5 pars. Online. Retrieved May 20, 2008, from Internet: http://pharos.bu.edu/Egypt/Wonders/Forgotten/greatwall.html

Sources: Reporters Without Borders, The OpenNet Initiative, China Internet Network Information Center , (2006). China and internet censorship. Retrieved May 12, 2008, from www.cnn.com Web site: http://www.cnn.com/interactive/world/0603/explainer.china.internet/frameset.exclude.html

Stirland, S (2008, May 20). Cisco Leak: Great firewall of China was a chance to sell more routers. Retrieved May 23, 2008, from Wired Blog Network Web site: http://blog.wired.com/27bstroke6/2008/05/leaked-cisco-do.html

Sullivan, D. (2006). Google created evil rank scale to decide on Chinese censorship, *Search Engine Watch*, January 30, 2006, Retrieved on May 23, 2008 from, http://blog.searchenginewatch.com/blog/060130-154414.

Taubman , G (1998). A Not -So World Wide Web: The Internet, China, and the Challenges to Nondemocratic Rule. *Political Communication, 15*, Retrieved May 20, 2008, from

http://www.ingentaconnect.com/content/routledg/upcp/1998/00000015/00000002/art00010

Thomas, Timothy L. (2004). *Dragon bytes; Chinese inofrmation-war theory and practice*. Fort Leavenworth, Kansas: Foreign Military Studies Office.

Thompson, C (2006). Google's china problem. *The New York Times*, Retrieved 5.23.08, from http://www.nytimes.com/2006/04/23/magazine/23google.html?ex=1145678400&en=8088370f09361283&ei=5087%0A

Valencia, L. (1998). Special Report lll - The Great Wall of China. Retrieved May 20, 2008, from Internet: http://www.mabuhay.com/BalitaL/National_News/X0040_Special_Report_lll_-.htm

XIAO, Qiang, Recent *Mechanisms of State Control Over the Chinese Internet, Presentation*, Retrieved 5/12/08, from http://www.uscc.gov/hearings/2007hearings/written_testimonies/07_07_31wrts/07_07_31_qiang_statement.php

Yi Feng, 1997. "Democracy, Political Stability and Economic Growth," *British Journal of Political Science*, volume 27.

Vita

Major Michael D. Whiting was born in Greeley, Colorado and was raised in Grand Junction, Colorado until the age of 22 when he enlisted into the United States Air Force as a communications operator. He went on to receive his Bachelor of Arts in Computer Information Systems in 1995. After seven years of enlisted service, he was selected for Officer Training School in 1996 and was commissioned to be a communications and computer officer. He currently has over 19 years military experience in a variety of communications and training jobs in the United States Air Force.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
19-06-2008	Master's Graduate Research Project	May 2007 – June 2008

4. TITLE AND SUBTITLE

THE GREAT FIREWALL OF CHINA: A CRITICAL ANALYSIS

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Michael D. Whiting

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/ICW/ENG/08-12

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

This space intentionally left blank.

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

None

14. ABSTRACT

Censorship has a great impact on society as we enter the cyber environment. The Chinese "Great Firewall", as it is commonly called, brings great attention to China as they enter into the global economy. The Great Firewall is one approach China tries to censor their people. Many techniques are used to establish this cyber boundary such as: firewalls, real-name internet registration, filtering, political controls, police actions and governmental controls. These controls are being challenged by Chinese nationals through the mass public, technology, and software. There are many political, diplomatic, international, and non-governmental organizations who continue their efforts to minimize the effects of the Great Firewall. The United States finds itself in a unique situation trying to eliminate human rights violations while encouraging freedom. Some United States companies find themselves in a moral dilemma; accept the Chinese requirements to do business which may include supporting censorship and human rights violations or to eliminate doing business with the Chinese and missing out on a great financial opportunity.

15. SUBJECT TERMS

Censorship, firewall, cyberspace

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Robert F. Mills, PhD
U	U	U	UU	50	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636, ext 4527 (robert.mills@afit.edu)